IN THE CLAIMS:

Please amend the claims as follows:

1. (Currently Amended) A method for protecting a data file on a computer system, comprising the steps of:

B1

providing a grantee's encryption key, a grantee's decryption key, a grantor's encryption key, and a grantor's decryption key;

using asymmetric encryption, encrypting the data file using ~~a~~ the grantor's encryption ~~private~~ key to create an encrypted data file;

~~generating a new key;~~

generating a transformation key from the ~~old~~ grantor's decryption key, ~~and~~ the ~~new~~ grantee's encryption key and other data which is data file independent;

~~updating~~ transforming the encrypted data file with the transformation key to ~~create~~ generate ~~an updated~~ a transformed encrypted data file wherein the transforming of the encrypted data file does not reveal the data file during the process of transforming;

~~replacing the encrypted data file with the updated~~ providing the transformed encrypted data file to the grantee; and

~~replacing the private key with the new key~~ decrypting the transformed encrypted file by the grantee with the grantee's decryption key;

wherein the ~~updating of the encrypted data file with the~~ transformation key does not ~~reveal the data file during the file during the process of updating~~ allow the grantee to determine the grantor's decryption key.

2. (Currently Amended) The method of claim 1, further comprising the step of repeating the ~~updating~~ generating step, and transforming step and the ~~two replacing steps~~ providing step on a periodic basis.

3. (Cancelled)

4. (Currently Amended) A processor-driven system adapted to protect a data file, the

system comprising:

a processor; and

a memory coupled to the processor for storing the data file;

wherein the processor is programmed to perform the steps of:

providing a grantee's encryption key, a grantee's decryption key, a grantor's encryption key, and a grantor's decryption key;

using asymmetric encryption, encrypting the data file using ~~a~~ the grantor's encryption ~~private~~ key to create an encrypted data file;

~~generating a new key~~;

generating a transformation key from the ~~old~~ grantor's decryption key, ~~and~~ the ~~new~~ grantee's encryption key and other data which is data file independent;

~~updating~~ transforming the encrypted data file with the transformation key to ~~create~~ generate ~~an updated~~ a transformed encrypted data file wherein the transforming does not reveal the data file during the process of transforming;

~~replacing the encrypted data file with the updated~~ providing the transformed encrypted data file to the grantee; and

~~replacing the private key with the new key~~ decrypting the transformed encrypted file by the grantee with the grantee's decryption key;

wherein the ~~updating of the encrypted data file with the~~ transformation key does not ~~reveal the data file during the process of updating~~ allow the grantee to determine the grantor's decryption key.

5. (Original) The processor-driven system of claim 4, further comprising a communication interface.

6. (Original) The processor-driven system of claim 4, wherein the processor and the memory are included within a portable device.

7. (Original) The processor-driven system of claim 4, wherein the processor and the memory are included within a smart card.

8. (Newly Presented) The method of claim 1, wherein said generating step comprises generating the transformation key from the grantor's decryption key, the grantee's encryption key, and the ciphertext of the encrypted data file.

9. (Newly Presented) The method of claim 1 wherein said generating step comprises generating the transformation key from the grantor's decryption key, the grantee's encryption key, and a random variable.

10. (Newly Presented) The method of claim 1 wherein said generating step comprises generating the transformation key from the grantor's decryption key, the grantee's encryption key, the ciphertext of the encrypted data file, and a random variable.

11. (Newly Presented) The processor driven system of claim 4, wherein said generating step comprises generating the transformation key from the grantor's decryption key, the grantee's encryption key, and the ciphertext of the encrypted data file.

12. (Newly Presented) The processor driven system of claim 4, wherein said generating step comprises generating the transformation key from the grantor's decryption key, the grantee's encryption key, and a random variable.

13. (Newly Presented) The processor driven system of claim 4, wherein said generating step comprises generating the transformation key from the grantor's decryption key, the grantee's encryption key, the ciphertext of the encrypted data file, and a random variable.